云数据库 TaurusDB

产品介绍

文档版本 01

发布日期 2024-11-29

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 什么是云数据库 TaurusDB 企业版

云数据库TaurusDB企业版是华为自研的最新一代企业级高扩展高性能云原生数据库，完全兼容MySQL。基于华为最新一代DFV存储，采用计算存储分离架构，128TB的海量存储，故障秒级切换，既拥有商业数据库的高可用和性能，又具备开源低成本效益。

TaurusDB企业版支持的版本请参见**TaurusDB引擎和版本**。

云数据库TaurusDB支持企业版和标准版两种产品形态。标准版请参见**什么是云数据库TaurusDB标准版**。

成长地图

您可以通过**成长地图**快速了解TaurusDB的相关概念、入门使用、高手进阶等。

如何使用 TaurusDB

您可以通过如下方式使用TaurusDB。

管理控制台：您可以使用**管理控制台**为您提供的Web界面完成TaurusDB的相关操作。

了解**TaurusDB产品优势**可以帮助您更好地选购TaurusDB。

产品优势

- 性能强悍
  - 采用计算与存储分离，日志即数据架构，性能提升至开源MySQL的7倍。
  - 通过RDMA协议进行数据库传输，使IO性能不再成为瓶颈。
  - 引入内核特性，例如Query result cache、Query plan cache、Online DDL等，提升用户体验。
- 弹性扩展
  - 横向扩展：1写15只读节点，快速添加只读节点，满足高并发场景性能需求。
  - 纵向扩展：分钟级规格升降级，轻松应对业务高峰。
- 高可靠性
  - 支持跨可用区部署，跨区域备份，提升实例容灾能力。
  - 存储三副本，数据更安全。

  - 共享分布式存储，主节点故障时，只读节点自动升级成主节点，RPO为0。
  - 主从节点时延支持ms级，保证业务高可用。
- 安全防护
  - 采用共享分布式存储，故障秒级恢复，数据“0”丢失。
  - 采用VPC、安全组、SSL连接和数据加密等严格控制安全访问。
  - 已通过ISO 27001、CSA、可信云、等保三级等国内外15+安全认证，国内首家获得NIST CSF最高认证。
- 高兼容性：

  完全兼容MySQL，应用无需改造即可轻松迁移上云。
- 高效备份
  - 全量备份采用快照机制，秒级完成创建快照，具有更高的备份效率。
  - 基于底层存储系统的多时间点特性，不需增量日志回放，可直接实现按时间点回滚。
- 海量存储
  - 华为自研DFV分布式存储，容量高达128TB。
  - 根据数据量自动伸缩，无须提前规划，节约成本。
- 算子下推

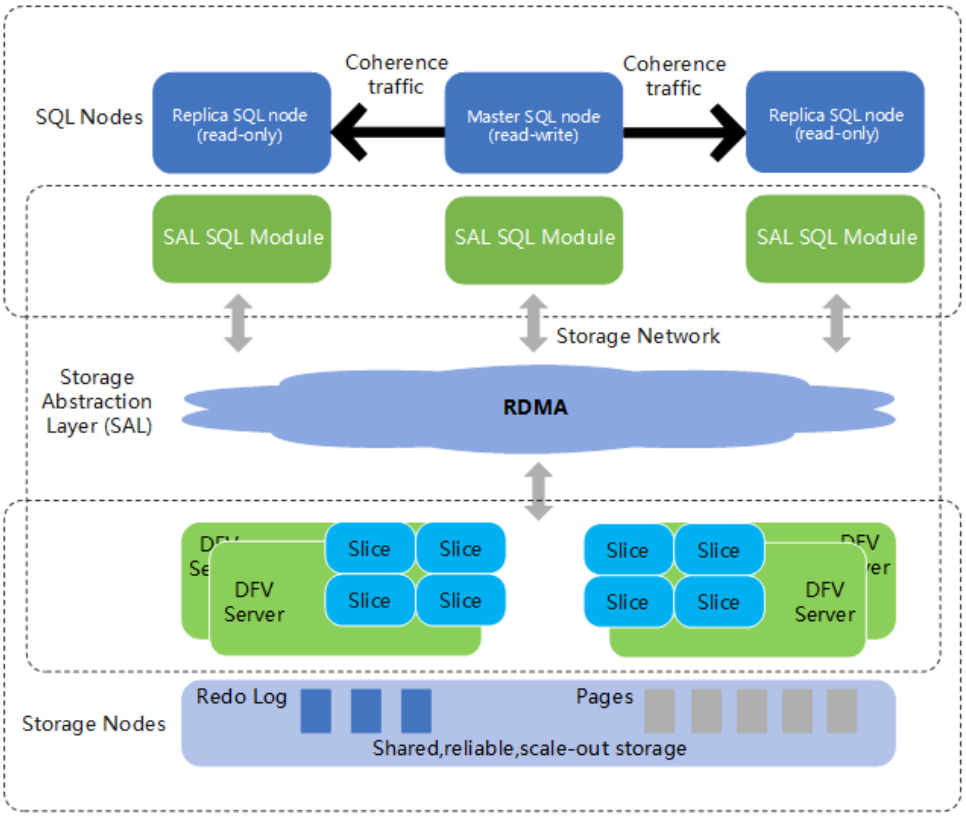
  将过滤条件、列投影、聚合运算从计算节点下推到存储节点，跨存储节点并行处理，减少网络流量和计算节点的压力，提升查询执行效率。同时与并行查询功能进行融合，达成全流程并行执行。

2 TaurusDB 产品架构

云数据库TaurusDB整体架构自下向上分为三层。

1. 存储层： 基于华为DFV存储，提供分布式、强一致和高性能的存储能力，此层来保障数据的可靠性以及横向扩展能力，保证数据的可靠性不低于99.999999999%。DFV（Data Function Virtualization）是一个与数据库垂直整合的高性能，高可靠的分布式存储系统。存储集群采取池化部署，可以有效提升存储使用效率，构建以数据为中心的全栈数据服务架构的解决方案。
2. 存储抽象层（Storage Abstraction Layer）：将原始数据库基于表文件的操作抽象为对应分布式存储，向下对接DFV，向上提供高效调度的数据库存储语义，是数据库高性能的核心。
3. SQL解析层：与MySQL 8.0开源版100%兼容，客户业务从MySQL生态可以平滑迁移， 从其他数据库迁移也能使用MySQL生态的语法、工具，降低开发、学习成本。基于原生MySQL，在100%兼容的前提下进行大量内核优化以及开源加固。

图 2-1 架构图



3 TaurusDB 常用概念

了解以下概念，有助于您更好地选购和使用TaurusDB。

集群实例

标准存储计算分离架构，支持1写15读，最高支持128TB存储容量，支持只读节点分钟级扩展。

单机实例

仅有1个主节点，没有只读节点。单机版无需处理多个节点之间的同步协作，易满足ACID事务需求。单机实例无高可用保障，出现故障后，无法保障及时恢复。

规格

每个节点的资源配置，比如16核64GB。

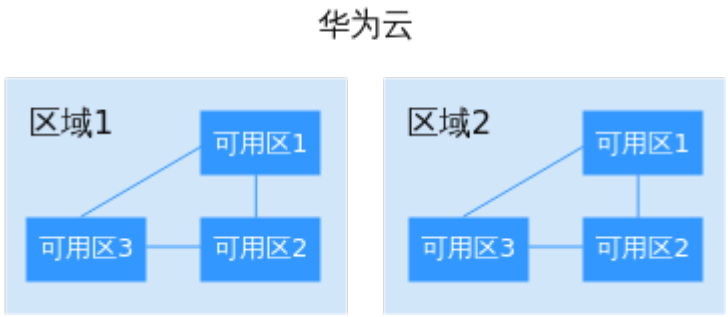
区域和可用区

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图3-1阐明了区域和可用区之间的关系。

图 3-1 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。更多信息请参见**华为云全球站点**。

浏览器

TaurusDB对浏览器的兼容性，详见**浏览器兼容性一览表**。

4 TaurusDB 产品优势

TaurusDB为计算存储分离、云化架构的企业级云数据库。

超高性能

对于某些业务负载，吞吐量最高可提升至开源MySQL7倍，可达百万级QPS。

高扩展性

- 横向扩展：支持分钟级添加只读节点，最大支持15只读，解决性能扩展问题。
- 纵向扩展：支持规格升级，应对不确定的业务增长。
- 存储扩展：根据数据容量自动弹性伸缩，无须提前规划容量，最大支持128TB，解决海量数据问题。

高可靠性

支持跨AZ部署、异地容灾，金融级别可靠性。

跨AZ部署，数据三副本，安全性有保障。

高兼容性

100%兼容MySQL，应用上云无须改造。

超低成本

十分之一的商用数据库成本。

非中间件式架构

业务性能正常情况下，无需搭载分布式数据库中间件分库分表。

5 实例说明

5.1 TaurusDB 引擎和版本

TaurusDB目前支持的数据库引擎和版本如表5-1所示。

表 5-1 数据库引擎和版本

数据库引擎	兼容的数据库版本	支持的内核小版本
TaurusDB	MySQL 8.0	• 2.0.54.240900 • 2.0.54.240600 • 2.0.51.240300 • 2.0.48.231200 • 2.0.45.230900 • 2.0.42.230600 • 2.0.39.230300 • 2.0.28.18 • 2.0.28.17 • 2.0.28.16 • 2.0.28.15 • 2.0.28.12 • 2.0.28.10 • 2.0.28.9 • 2.0.28.7 • 2.0.28.4 • 2.0.28.1

说明

关于各个内核小版本的更新说明请参见**内核版本发布说明**。

5.2 TaurusDB 实例规格

TaurusDB实例的CPU架构分为X86架构和鲲鹏架构。

- X86架构：搭载英特尔®至强®可扩展处理器，配套高性能网络，综合性能及稳定性全面提升，满足对业务稳定性及计算性能要求较高的企业级应用。
- 鲲鹏架构：搭载鲲鹏920处理器及25GE智能高速网卡，提供强劲的鲲鹏算力和高性能网络，能更好地满足各类企业对云上业务高性价比、安全可靠等需求。

不同的CPU架构支持的数据库实例规格不同，具体如下：

X86 架构实例规格

X86架构的实例规格支持两种子系列：独享型规格和通用型规格。

- **独享型**：完全独享的CPU和内存，性能长期稳定，不会因为物理机上其他实例的行为而受到影响。适用于对性能稳定性要求较高的应用场景。

  独享型实例支持的区域如下：华北-北京四、华东-上海一、华南-广州、华南-广州-友好用户环境、西南-贵阳一、华北-乌兰察布一、亚太-新加坡、亚太-雅加达、土耳其-伊斯坦布尔、拉美-圣保罗一。
- **通用型**：与同一物理机上的其他通用版规格实例共享CPU和内存，通过资源复用换取CPU使用率最大化，性价比较高。适用于对性能稳定性要求较低的应用场景。

  支持的区域如下：华北-北京四、华东-上海一、华南-广州。

表 5-2 X86 架构实例规格

规格类型	规格码	vCPU（个）	内存（GB）
独享型	gaussdb.mysql.large.x86.4	2	8
	gaussdb.mysql.large.x86.8	2	16
	gaussdb.mysql.xlarge.x86.4	4	16
	gaussdb.mysql.xlarge.x86.8	4	32
	gaussdb.mysql.2xlarge.x86.4	8	32
	gaussdb.mysql.2xlarge.x86.8	8	64
	gaussdb.mysql.4xlarge.x86.4	16	64
	gaussdb.mysql.4xlarge.x86.8	16	128
	gaussdb.mysql.8xlarge.x86.4	32	128
	gaussdb.mysql.8xlarge.x86.8	32	256

规格类型	规格码	vCPU（个）	内存（GB）
	gaussdb.mysql.16xlarge.x86.4	60	256
	gaussdb.mysql.16xlarge.x86.8	64	512
通用型	gaussdb.mysql.large.x86.normal.4	2	8
	gaussdb.mysql.xlarge.x86.normal.2	4	8
	gaussdb.mysql.xlarge.x86.normal.4	4	16
	gaussdb.mysql.2xlarge.x86.normal.2	8	16
	gaussdb.mysql.2xlarge.x86.normal.4	8	32
	gaussdb.mysql.4xlarge.x86.normal.2	16	32
	gaussdb.mysql.4xlarge.x86.normal.4	16	64
	gaussdb.mysql.8xlarge.x86.normal.2	32	64
	gaussdb.mysql.8xlarge.x86.normal.4	32	128

须知

- 数据库实例规格请以实际环境为准。
- TPS和QPS性能数据，请参见《**性能白皮书**》。

鲲鹏架构实例规格

鲲鹏架构的实例规格支持独享型规格。

独享型：完全独享的CPU和内存，性能长期稳定，不会因为物理机上其他实例的行为而受到影响。适用于对性能稳定性要求较高的应用场景。

独享型实例支持的区域如下：华北-北京四、华东-上海一、华南-广州、华南-广州-友好用户环境、西南-贵阳一、华北-乌兰察布一、亚太-新加坡、亚太-雅加达、土耳其-伊斯坦布尔、拉美-圣保罗一。

表 5-3 鲲鹏架构实例规格

规格类型	规格码	vCPU（个）	内存（GB）
独享型	gaussdb.mysql.xlarge.arm.4	4	16
	gaussdb.mysql.xlarge.arm.8	4	32
	gaussdb.mysql.2xlarge.arm.4	8	32
	gaussdb.mysql.2xlarge.arm.8	8	64
	gaussdb.mysql.4xlarge.arm.4	16	64
	gaussdb.mysql.4xlarge.arm.8	16	128
	gaussdb.mysql.8xlarge.arm.4	32	128
	gaussdb.mysql.8xlarge.arm.8	32	256
	gaussdb.mysql.12xlarge.arm.4	48	192
	gaussdb.mysql.12xlarge.arm.8	48	384
	gaussdb.mysql.15xlarge.arm.8	60	480

须知

- 数据库实例规格请以实际环境为准。
- TPS和QPS性能数据，请参见《**性能白皮书**》。

5.3 TaurusDB 实例存储类型

TaurusDB提供DL6和DL5两种存储类型。

本章节主要介绍两种存储类型的区别，帮助您选择更符合业务场景的存储类型。

存储类型介绍

表 5-4 存储类型介绍

存储类型	特点	适用场景
DL6（Cloud Database Engine Level 6）	原“共享存储”。TaurusDB历史版本默认支持的存储类型，2024年7月前创建的实例默认的存储类型。 DL6存储类型的实例采用3AZ部署，RPO=0；性能更佳、峰值吞吐量更高。	对性能敏感，业务高峰对存储IO要求极高的核心应用系统，如金融、电商、政务和游戏等。
DL5（Cloud Database Engine Level 5）	TaurusDB全新推出的存储类型，底层基于华为云自研硬件及网络底座技术，保持了DL6的3AZ，RPO=0的高可用性，峰值性能有所下降，单位容量的成本显著降低。	CPU密集型的次核心业务系统；或有降低成本诉求，追求高性价比的应用模块。

说明

由于两类存储依托于不同物理介质，对于已创建的实例，存储类型无法支持直接切换。如需切换存储类型，建议您购买一个新的TaurusDB实例并配置预期的存储类型，将原有实例的数据通过DRS工具迁移到新实例上。

计费说明

- 中国内地区域的费用请参见**表5-5**。

  表 5-5 计费说明

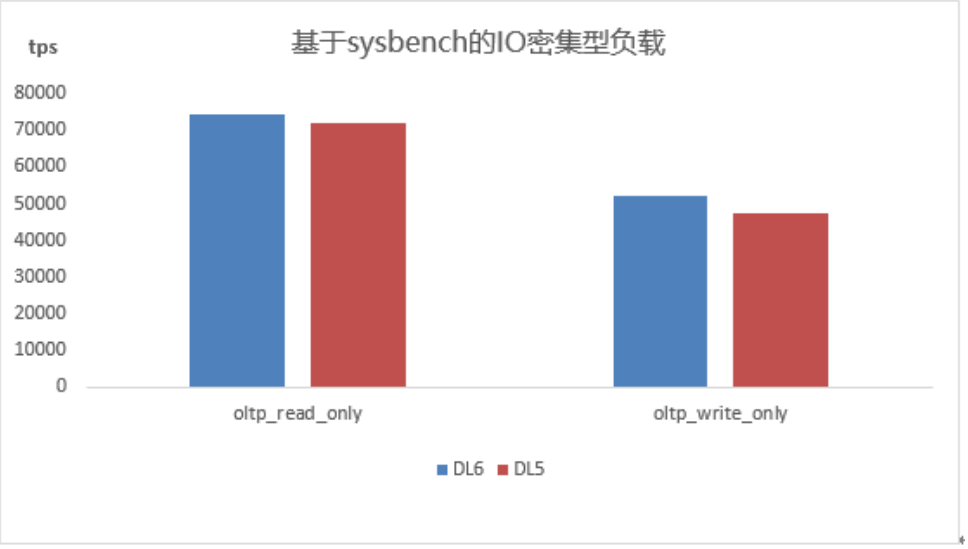
存储类型	按需费用	包月费用
DL6	0.00625 元/GB/小时	3 元/GB/月
DL5	0.00458 元/GB/小时	2.2 元/GB/月

- 中国香港及海外等其他区域的价格请参见**价格计算器**。

性能对比

在相同的计算规格下，基于sysbench基准测试方法，对比测试IO密集型负载下DL6和DL5实例的性能，只读性能差别在3%左右，只写性能差别在10%以内。

图 5-1 性能对比结果



5.4 TaurusDB 实例状态

数据库实例状态是数据库实例的运行情况。用户可以使用管理控制台查看数据库实例状态。

表 5-6 状态及说明

状态	说明
正常	数据库实例正常和可用。
异常	数据库实例不可用。
创建中	正在创建数据库实例。
创建失败	数据库实例创建失败。
重启中	正在重启数据库实例。
实例名称修改中	正在修改数据库实例名称。
端口修改中	正在修改数据库实例的数据库端口。
规格变更中	正在变更数据库实例的CPU和内存规格。
添加只读中	正在进行数据库实例添加只读节点。
删除只读中	正在进行数据库实例删除只读节点。
只读升主中	只读节点正在切换为主节点。
只读节点隔离中	只读节点正在进行隔离。
只读节点已隔离	只读节点完成隔离操作。
备份中	正在备份数据库实例。

状态	说明
扩容中	正在扩容数据库实例的磁盘空间。
冻结	账户余额小于或等于0元，系统对该用户下的实例进行冻结。您需前往费用中心进行充值，充值成功且欠款核销后，冻结保留期内的实例才会解冻。
证书配置变更中	正在进行数据库实例证书配置变更。
Serverless算力变更中	Serverless实例正在进行算力变更。
小版本升级中	正在进行数据库实例内核版本升级。
已删除	数据库实例已被删除，对于已经删除的实例，将不会在实例列表中显示。

6 安全

6.1 责任共担

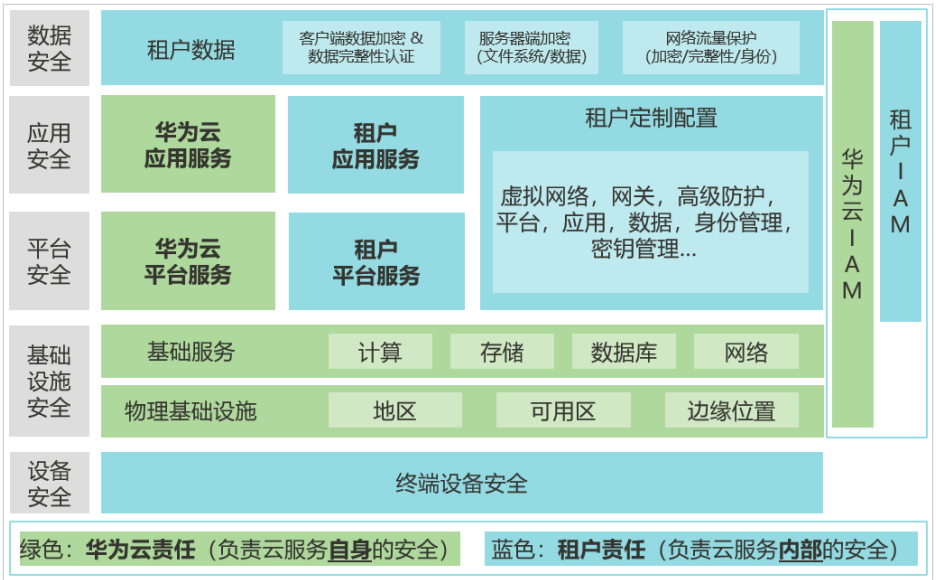
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如**图6-1**所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。 华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 6-1 华为云安全责任共担模型



6.2 身份认证与访问控制

身份认证

用户访问云数据库TaurusDB时支持对数据库用户进行身份验证，包含密码验证和IAM验证两种方式。

- **密码验证**

  您需要对数据库实例进行管理，使用数据管理服务（Data Admin Service）登录数据库时，需要对账号密码进行验证，验证成功后方可进行操作。

- **IAM验证**

  您可以使用**统一身份认证服务**（Identity and Access Management， IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全地控制华为云资源的访问。您创建的IAM用户，需要通过验证用户和密码才可以使用TaurusDB资源。具体请参见**创建IAM用户并登录**。

访问控制

- **权限控制**

  购买实例之后，您可以使用IAM为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，通过IAM进行精细的权限管理。具体内容请参见**TaurusDB权限管理**。

- **VPC和子网**

  虚拟私有云（Virtual Private Cloud， VPC）为云数据库构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云上资源的安全性，简化用户的网络部署。您可以在VPC中定义安全组、VPN、IP地址段、带宽等网络特性，方便管理、配置内部网络，进行安全、快捷的网络变更。

  子网提供与其他网络隔离的、可以独享的网络资源，以提高网络安全性。

  具体内容请参见**创建虚拟私有云和子网**。

- **安全组**

  安全组是一个逻辑上的分组，为同一个虚拟私有云内具有相同安全保护需求并相互信任的弹性云服务器和TaurusDB数据库实例提供访问策略。为了保障数据库的安全性和稳定性，在使用TaurusDB数据库实例之前，您需要设置安全组，开通需访问数据库的IP地址和端口。

6.3 数据保护技术

TaurusDB通过多种数据保护手段和特性，保障存储在TaurusDB中的数据安全可靠。

表 6-1 多种数据保护手段

数据保护手段	简要说明
传输加密（HTTPS）	支持HTTP和HTTPS两种传输协议，为保证数据传输的安全性，推荐您使用更加安全的HTTPS协议。
数据备份	支持设置数据库的备份和恢复，来保障数据的可靠性。
敏感操作保护	控制台支持敏感操作保护，开启后执行删实例等敏感操作时，系统会进行身份验证，进一步保证TaurusDB配置和数据的安全性。
SSL数据加密	可以使用SSL来加密数据库TaurusDB和客户端的连接。SSL通过互相认证、使用数字签名确保完整性、使用加密确保私密性，以实现客户端和服务器之间的安全通讯。

6.4 审计与日志

审计

- 云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

  CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

  通过云审计服务，您可以记录与TaurusDB实例相关的操作事件，便于日后的查询、审计和回溯。

- 数据库安全服务（Database Security Service，DBSS）

  DBSS是一个智能的数据库安全服务，基于机器学习机制和大数据分析技术，提供数据库审计，SQL注入攻击检测，风险操作识别等功能，保障云上数据库的安全。

  建议使用DBSS来提供扩展的数据安全能力，详情请参考**数据库安全服务**。

  优势：

  - 助力企业满足等保合规要求。
    - 满足等保测评数据库审计需求。
    - 满足国内外安全法案合规需求，提供满足数据安全标准（例如Sarbanes-Oxley）的合规报告。

- 支持备份和恢复数据库审计日志，满足审计数据保存期限要求。
- 支持风险分布、会话统计、会话分布、SQL分布的实时监控能力。
- 提供风险行为和攻击行为实时告警能力，及时响应数据库攻击。
- 帮助您对内部违规和不正当操作进行定位追责，保障数据资产安全。

数据库安全审计采用数据库旁路部署方式，在不影响用户业务的前提下，可以对数据库进行灵活的审计。

- 基于数据库风险操作，监视数据库登录、操作类型（数据定义、数据操作和数据控制）和操作对象，有效对数据库进行审计。
- 从风险、会话、SQL注入等多个维度进行分析，帮助您及时了解数据库状况。
- 提供审计报表模板库，可以生成日报、周报或月报审计报表（可设置报表生成频率）。同时，支持发送报表生成的实时告警通知，帮助您及时获取审计报表。

日志

出于分析或审计等目的，用户可以开启实例的日志记录功能。当用户开启日志记录功能后，TaurusDB可以通过管理控制台查看。

- 错误日志

  TaurusDB支持查看数据库级别的日志，包括数据库运行的错误信息，以及运行较慢的SQL查询语句，有助于您分析系统中存在的问题。

- 慢日志

  慢日志用来记录执行时间超过当前慢日志阈值“long_query_time”（默认是10秒）的语句，您可以通过查询慢日志的日志明细、统计分析情况，查找出执行效率低的语句，进行优化。

- 全量SQL

  当您开启全量SQL功能，系统会将所有的SQL文本内容进行存储，以便进行分析。

  TaurusDB默认关闭全量SQL功能。

  全量SQL打开后，可以通过数据库管理服务（Data Admin Service，DAS）查看SQL语句耗时信息，例如平均执行耗时、总耗时、 平均锁等待耗时、平均扫描行数等。

6.5 监控安全风险

云监控服务为用户提供一个针对云数据库、云服务器等资源的立体化监控平台。使您全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

监控指标

TaurusDB提供基于云监控服务的资源和操作监控能力，例如CPU使用率、网络吞吐量等。

监控指标周期目前支持1分钟、1秒、5秒，默认监控周期为1分钟。通过开启秒级监控可以提高监控指标的精确值。

事件监控

事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对TaurusDB的操作事件收集到云监控服务，并在事件发生时进行告警。

6.6 故障恢复

TaurusDB会在数据库实例的备份时段中创建数据库实例的自动备份。系统根据您指定的备份保留期（1-732天）保存数据库实例的自动备份。

跨区域备份

TaurusDB支持将备份文件存放到另一个区域存储，某一区域的实例故障后，可以在异地区域使用备份文件在异地恢复到新的TaurusDB实例，用来恢复业务。

实例开启跨区域备份策略后，会自动将该实例的备份文件备份到目标区域。

多可用区

可用区指在同一区域下，电力、网络隔离的物理区域，可用区之间内网互通，不同可用区之间物理隔离。TaurusDB支持将实例的节点分别部署在多个可用区，以此来实现跨可用区容灾能力。

故障转移

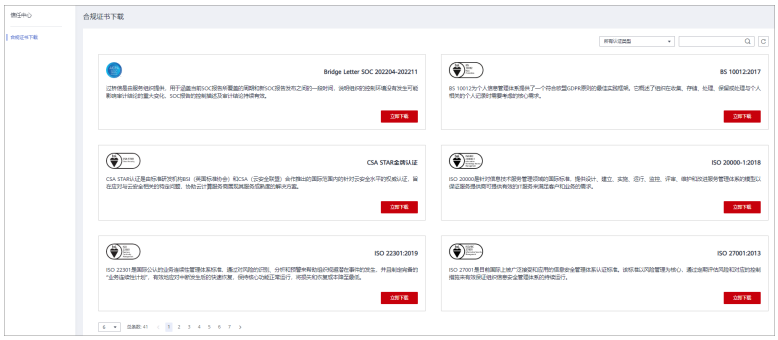
TaurusDB是一个多节点的实例，每个实例默认只有1个主节点，其余节点为只读节点。当主节点发生故障时，只读节点会自动升级为主节点，保证实例的可用性。

6.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 6-2 合规证书下载



资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 6-3 资源中心

销售许可证&软件著作权证书

另外，华为云还提供了以下销售许可证及软件著作权证书，供用户下载和参考。具体请查看**合规资质证书**。

图 6-4 销售许可证&软件著作权证书

7 TaurusDB 权限管理

如果您需要对华为云上购买云服务平台上创建的TaurusDB资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为账号中给员工创建IAM用户，并授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望开发人员拥有TaurusDB的使用权限，但是不希望他们拥有删除TaurusDB等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用TaurusDB，但是不允许删除TaurusDB的权限，控制他们对TaurusDB资源的使用范围。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用TaurusDB服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**IAM产品介绍**。

TaurusDB 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

TaurusDB部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京四）对应的项目（cn-north-4）中设置相关权限，并且该权限仅对此项目生效；如果在所有项目中设置权限，则该权限在所有区域项目中都生效。访问TaurusDB时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对TaurusDB服务，管理员能够控制IAM

用户仅能对某一类数据库资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，TaurusDB支持的API授权项请参见**策略及授权项说明**。

如**表7-1**所示，包括了云数据库TaurusDB的所有系统权限。

表 7-1 TaurusDB 系统权限

策略名称	描述	类别
GaussDB FullAccess	云数据库TaurusDB服务的所有执行权限。	系统策略。
GaussDB ReadOnlyAccess	云数据库TaurusDB服务的只读访问权限。	系统策略。

表7-2列出了云数据库TaurusDB常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 7-2 常用操作与系统权限的关系

操作	GaussDB FullAccess	GaussDB ReadOnlyAccess
创建TaurusDB实例	支持	不支持
删除TaurusDB实例	支持	不支持
查询TaurusDB实例列表	支持	支持

表 7-3 常用操作与对应授权项

操作名称	授权项	备注
修改参数模板	gaussdb:param:modify	-
变更数据库实例的规格	gaussdb:instance:modifySpec	-

操作名称	授权项	备注
创建数据库实例	gaussdb:instance:create	界面选择VPC、子网、安全组需要配置： vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get 创建加密实例需要在项目上配置KMS Administrator权限。 创建包周期实例需要配置CBC权限： bss:renewal:view bss:renewal:update bss:balance:view bss:order:view bss:order:update bss:order:pay 创建TDE实例时，需要配置授予创建服务关联委托的权限：iam:agencies:createServiceLinkedAgencyV5。
创建手动备份	gaussdb:backup:create	-
查询备份列表	gaussdb:backup:list	-
查询错误日志	gaussdb:log:list	-
重启实例	gaussdb:instance:restart	-
查询数据库实例列表	gaussdb:instance:list	-
创建参数模板	gaussdb:param:create	-
删除参数模板	gaussdb:param:delete	-
修改备份策略	gaussdb:instance:modifyBackupPolicy	-
查看参数模板	gaussdb:param:list	-
删除实例	gaussdb:instance:delete	退订包周期实例需要配置： bss:unsubscribe:update
删除手动备份	gaussdb:backup:delete	-
查询项目标签	gaussdb:tag:list	-

操作名称	授权项	备注
应用参数模板	gaussdb:param:apply	-
批量添加删除项目标签	gaussdb:instance:dealTag	-
变更配额	gaussdb:quota:modify	-
升级数据库实例版本	gaussdb:instance:upgrade	-
只读升主	gaussdb:instance:switchover	-
修改数据库端口	gaussdb:instance:modifyPort	-
修改实例安全组	gaussdb:instance:modifySecurityGroup	-
修改读写内网地址	gaussdb:instance:modifyIp	界面选择IP需要配置： vpc:vpcs:list vpc:vpcs:get
开启、关闭SSL	gaussdb:instance:modifySSL	-
修改实例名称	gaussdb:instance:rename	-
添加只读节点	gaussdb:instance:addNodes	-
删除只读节点	gaussdb:instance:deleteNodes	-
修改存储空间	gaussdb:instance:modifyStorageSize	-
修改数据库实例密码	gaussdb:instance:modifyPassword	-
绑定公网IP	gaussdb:instance:bindPublicIp	界面列出公网IP需要配置： vpc:publicIps:get vpc:publicIps:list
解绑公网IP	gaussdb:instance:unbindPublicIp	-
修改监控策略	gaussdb:instance:modifyMonitorPolicy	-
修改节点倒换优先级	gaussdb:instance:modifySwitchoverPriority	-
修改可维护时间窗	gaussdb:instance:modifyMaintenanceWindow	-

操作名称	授权项	备注
节点隔离	gaussdb:instance:isolateNodes	-
修改全量SQL策略	gaussdb:instance:modifyTraceSQLPolicy	-
查询HTAP实例列表	gaussdb:htapInstance:list	-
创建HTAP实例	gaussdb:htapInstance:create	-
修改云数据库 GaussDB HTAP实例	gaussdb:htapInstance:modify	-
删除HTAP实例	gaussdb:htapInstance:delete	-
修改HTAP实例名称	gaussdb:htapInstance:rename	-
重启HTAP实例	gaussdb:htapInstance:restart	-
升级HTAP实例版本	gaussdb:htapInstance:upgrade	-
倒换HTAP实例	gaussdb:htapInstance:switchover	-
变更HTAP实例的规格	gaussdb:htapInstance:modifySpec	-
扩容HTAP实例磁盘空间	gaussdb:htapInstance:modifyStorageSize	-
绑定HTAP实例公网IP	gaussdb:htapInstance:bindPublicIp	-
解绑HTAP实例公网IP	gaussdb:htapInstance:unbindPublicIp	-
修改HTAP实例端口	gaussdb:htapInstance:modifyPort	-
修改HTAP实例密码	gaussdb:htapInstance:modifyPassword	-
创建HTAP实例数据同步	gaussdb:htapInstance:createDataSync	-
修改HTAP实例数据同步	gaussdb:htapInstance:modifyDataSync	-
删除HTAP实例数据同步	gaussdb:htapInstance:deleteDataSync	-

操作名称	授权项	备注
创建数据库代理	gaussdb:proxy:create	-
修改代理地址	gaussdb:proxy:modifyIp	-
修改数据库代理读权重	gaussdb:proxy:modifyWeight	-
修改数据库代理端口	gaussdb:proxy:modifyPort	-
修改数据库代理访问控制	gaussdb:proxy:modifyAccess	-
删除数据库代理	gaussdb:proxy:delete	-
查询数据库代理列表	gaussdb:proxy:list	-
升级数据库代理版本	gaussdb:proxy:upgrade	-
修改数据库代理名称	gaussdb:proxy:rename	-
扩容数据库代理节点	gaussdb:proxy:addNodes	-
缩容数据库代理节点	gaussdb:proxy:deleteNodes	-
变更数据库代理规格	gaussdb:proxy:modifySpec	-
申请数据库代理内网域名	gaussdb:proxy:createDns	-
修改数据库代理域名	gaussdb:proxy:modifyDns	-
删除数据库代理域名	gaussdb:proxy:deleteDns	-
修改数据库代理路由模式	gaussdb:proxy:modifyRouteMode	-
修改数据库代理SSL	gaussdb:proxy:modifySSL	-
创建数据库用户	gaussdb:user:create	-
删除数据库用户	gaussdb:user:delete	-
修改数据库用户密码	gaussdb:user:modify	-
查询数据库用户	gaussdb:user:list	-
数据库用户授权	gaussdb:user:grantPrivilege	-
回收数据库用户权限	gaussdb:user:revokePrivilege	-
创建数据库	gaussdb:database:create	-
删除数据库	gaussdb:database:delete	-
查询数据库列表	gaussdb:database:list	-

操作名称	授权项	备注
查询预定义标签	-	查询预定义标签需要配置： tms:resourceTags:list
查询配置日志组	-	查询配置日志组需要配置： lts:groups:get
查询配置日志流	-	查询配置日志流需要配置： lts:topics:get
设置自动变配	gaussdb:autoscaling:createPolicy	设置自动变配需要配置： iam:agencies:listAgencies

8 TaurusDB 约束与限制

TaurusDB在使用上有一些固定限制，用来提高实例的稳定性和安全性。

规格与性能限制

表 8-1 规格与性能限制

资源类型	限制	说明
存储空间大小	• 按需实例：最大128000GB。 • 包年/包月实例：40GB~128000GB。 • Serverless实例：最大128000GB。 • 标准版HTAP实例：BE节点50GB~32000GB，FE节点50GB~1000GB。	-
临时盘空间大小	最大500GB。	更多关于临时盘的使用请参见**TaurusDB的临时盘使用说明**。
连接数	TaurusDB服务对此未做限制，取决于数据库引擎参数的默认值和取值范围。	更多关于最大连接数的内容请参见**TaurusDB数据库实例支持的最大连接数是多少**。

配额限制

表 8-2 配额限制

配额	限制	说明
TaurusDB实例	TaurusDB实例数量限制为50个。	如需更多配额，请参见**申请扩大配额**。

配额	限制	说明
只读节点	• 单个“包年/包月”实例：可创建0~15个只读节点。 • 单个“按需计费”实例：可创建0~15个只读节点。 • 单个“Serverless”实例：可创建0~7个只读节点。	更多信息，请参见**TaurusDB只读节点简介**。
标签	每个实例最多支持20个标签配额。	更多信息，请参见**TaurusDB标签管理**。
免费备份空间	免费赠送部分存储空间，其总容量约为购买的存储容量的100%。	更多信息，请参见**TaurusDB的备份是如何收费的**。
自动备份保留天数	• 同区域备份：默认为7天，可选择范围为1～732天。可联系客服申请开通至最大3660天。 • 跨区域备份：1～1825天。	更多信息，请参见**设置同区域备份策略**和**设置跨区域备份策略**。
日志保留天数	• 错误日志明细：30天 • 慢日志明细：30天 • 慢日志明文显示：30天	更多信息，请参见**日志管理**。

命名限制

表 8-3 命名限制

限制项	限制	说明
实例名称	长度在4个到64个字符之间，必须以字母开头，可以包含字母、数字、中划线或下划线，不能包含其他特殊字符。	更多信息请参见**修改实例名称**。
数据库名称	• 长度在1～64个字符之间，由字母、数字、下划线、中划线组成，中划线累计出现的次数不能超过10次，且不能包含其他特殊字符。 • 不能使用保留关键字，防止报错。具体请参见**保留关键字**。	更多信息请参见**创建数据库**。
账号名称	• 长度在1~32个字符之间，由字母、数字、下划线组成，不能包含其他特殊字符。 • 不能使用保留关键字，防止报错。具体请参见**保留关键字**。	更多信息请参见**创建数据库账号**。

限制项	限制	说明
参数模板名称	长度在1~64个字符之间，区分大小写，可包含字母、数字、中划线、下划线或句点，不能包含其他特殊字符。	更多信息请参见**创建参数模板**。
备份名称	长度在4个到64个字符之间，必须以字母开头，可以包含字母、数字、中划线或下划线，不能包含其他特殊字符。	更多信息请参见**创建手动备份**。
表名/函数名/存储过程名/视图名	不能使用保留关键字，防止报错。具体请参见**保留关键字**。	更多信息请参见**库表设计规范**。

安全限制

表 8-4 安全限制

限制项	限制	说明
数据库的root权限	创建实例页面只提供管理员root账户。	-
账号密码	• 长度为8~32个字符。 • 至少包含以下字符中三种：大写字母、小写字母、特殊字符~!@#$%^*-_=+?,()&|.和数字。 • 不能与用户名或倒序的用户名相同。 • 需要符合validate_password相关参数的设定值。 您可以单击实例名称，在左侧导航栏选择“参数修改”，在页面右上方搜索“validate_password”，查看密码相关参数值。	更多信息请参见**重置管理员密码**。
端口	• 默认为3306，允许手动修改。 • 数据库端口设置范围为1025～65534，其中5342、5343、5344、5345、12017、20000、20201、20202、33060、33062和33071被系统占用不可设置。	更多信息请参见**修改数据库端口**。
虚拟私有云 VPC	目前TaurusDB实例创建完成后不支持切换虚拟私有云。	-

限制项	限制	说明
安全组	• 默认情况下，一个用户可以创建100个安全组。 • 默认情况下，一个安全组最多只允许拥有50条安全组规则。 • 目前一个TaurusDB实例允许绑定多个安全组，一个安全组可以关联多个TaurusDB实例。 • 创建实例时，可以选择多个安全组（为了更好的网络性能，建议不超过5个）。	-
系统账号	创建TaurusDB实例时，系统会自动为实例创建如下系统账户（用户不可使用），用于给数据库实例提供完善的后台运维管理服务。 • rdsAdmin：管理账户，拥有最高权限，用于查询和修改实例信息、故障排查、迁移、恢复等操作。 • rdsRepl：复制账户，用于备实例或只读实例在主实例上同步数据。 • rdsBackup：备份账户，用于后台的备份。 • rdsMetric：指标监控账户，用于watchdog采集数据库状态数据。 • rdsProxy：数据库代理账户，该账户在开通读写分离时才会自动创建，用于通过数据库代理地址连接数据库时鉴权使用。	-
实例参数	大部分参数可以通过控制台或API进行修改，同时为了保证实例安全稳定运行，部分参数不支持修改。	更多信息请参见**修改TaurusDB实例参数**。

实例操作限制

表 8-5 功能使用限制

限制项	限制	说明
MySQL存储引擎	TaurusDB只支持InnoDB存储引擎。	-

限制项	限制	说明
访问TaurusDB	• 如果TaurusDB实例没开通公网访问，则该实例必须与弹性云服务器在同一个虚拟私有云内才能访问。 • 弹性云服务器必须处于目标TaurusDB实例所属安全组允许访问的范围内。 如果TaurusDB实例与弹性云服务器处于不同的安全组，系统默认不能访问。需要在TaurusDB实例的安全组添加一条“入”的访问规则。 “入”规则开放TCP协议，使用实例的默认端口。 • TaurusDB实例的端口： 默认端口为3306，需用户手动修改端口号后，ECS或外网才能访问其他端口。具体操作请参见**修改数据库端口**。	-
数据迁移	使用DRS或mysqldump迁移到TaurusDB数据。	更多信息请参见**数据迁移**。
重启TaurusDB实例	无法通过命令行重启，必须通过TaurusDB的管理控制台重启实例。	更多信息请参见**重启实例**。
查看TaurusDB备份	TaurusDB数据库实例在对象存储服务上的备份文件，对用户不可见。	-
开启Binlog	TaurusDB不支持只读节点开启Binlog。	更多信息请参见**TaurusDB如何开启并查看Binlog文件？**。
分区表	TaurusDB现有产品能力和社区8.0.22版本是兼容的，对于分区表，如果是list分区，目前每个分区的values最多只支持256个，超出会报错。（规避措施：将values个数过多的分区拆成更小的分区，确保每个分区的values个数都不超过256个。）	-
小规格实例	对于2U8GB的TaurusDB实例，单个实例中总的表数量不能超过30万个，单个数据库中的表数量不能超过5000个。	-

9 TaurusDB 与其他服务的关系

TaurusDB与其他服务之间的关系，具体表9-1所示。

表 9-1 与其他服务的关系

相关服务	交互功能
弹性云服务器（ECS）	TaurusDB配合弹性云服务器（Elastic Cloud Server，简称ECS）一起使用，通过内网连接TaurusDB可以有效地降低应用响应时间、节省公网流量费用。
虚拟私有云（VPC）	对您的TaurusDB数据库实例进行网络隔离和访问控制。
对象存储服务（OBS）	存储您的TaurusDB数据库实例的自动和手动备份数据。
云监控服务（Cloud Eye）	云监控服务是一个开放性的监控平台，帮助用户实时监测TaurusDB资源的动态。云监控服务提供多种告警方式以保证及时预警，为您的服务正常运行保驾护航。
云审计服务（CTS）	云审计服务（Cloud Trace Service，简称CTS），为用户提供云服务资源的操作记录，供您查询、审计和回溯使用。
数据复制服务（DRS）	使用数据复制服务，实现数据库平滑迁移上云。
企业管理服务（EPS）	企业管理服务（Enterprise Project Management Service，简称EPS）提供统一的云资源按企业项目管理，以及企业项目内的资源管理、成员管理。
标签管理服务（TMS）	标签管理服务（Tag Management Service，简称TMS）是一种快速便捷将标签集中管理的可视化服务，提供跨区域、跨服务的集中标签管理和资源分类功能。
分布式数据库中间件（DDM）	对于云数据库TaurusDB，使用分布式数据库中间件服务（Distributed Database Middleware，简称DDM），后端对接多个数据库实例，实现分布式数据库的透明访问。

10 TaurusDB 与 RDS for MySQL 的区别

TaurusDB拥有较好的性能、扩展性和易用性，详情请参见表10-1。

表 10-1 TaurusDB 与 RDS for MySQL 的差异

类别	RDS for MySQL	TaurusDB
架构	传统主备架构，主备通过binlog同步数据。	存算分离架构，计算节点共享一份数据，无需通过binlog同步数据。
性能	十万级QPS，高并发场景下性能提升3倍。	支持百万级QPS；对于某些业务负载，吞吐量最高可提升至开源MySQL7倍；复杂查询场景，支持将提取列、条件过滤、聚合运算等操作向下推给存储层处理，性能相比传统架构提升数十倍。
扩展性	• 最多添加5个只读节点，添加只读所需时间与数据量大小相关，并且需要增加一份存储。 • 存储自动扩容，最大支持4TB。	• 最多添加15只读，由于共享存储，添加只读节点所需时间与数据量大小无关，且无需增加一份存储。 • 存储自动扩容，最大支持128TB。
可用性	故障自动倒换，RTO通常小于30秒。	主节点和只读节点无需通过binlog进行数据同步，延时更低，故障自动切换，RTO通常小于10秒。
备份恢复	通过全量备份+binlog回放实现任意时间点回滚。	通过全量备份（快照）+redo回放实现任意时间点回滚，备份恢复速度更快。
数据库版本	MySQL 5.6、5.7和8.0。	MySQL 8.0。